Freeform Search

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Term: L11 not 17

Display: 10 **Documents in Display Format:** - **Starting with Number** 1

Generate: ○ **Hit List** ● **Hit Count** ○ **Side by Side** ○ **Image**

Search Clear Interrupt

Search History

DATE: Tuesday, August 02, 2005 Printable Copy Create Case

Set Name side by side	**Query**	**Hit Count**	**Set Name** result set
	DB=PGPB,USPT,USOC; THES=ASSIGNEE; PLUR=YES; OP=OR		
L12	L11 not 17	14	L12
L11	L10 and 12	15	L11
L10	L9 and rating	15	L10
L9	L8 and 15	137	L9
L8	(smart adj card) or ("smart-card") or smartcard	17624	L8
L7	L6 and rating	10	L7
L6	L5 and clearance	80	L6
L5	L4 or 13	873	L5
L4	L2 and @pd<=20011012	484	L4
L3	L2 and @ad<=20011012	850	L3
L2	("CHECK-IN" or boarding) and security	1934	L2
	DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR		
L1	6119096.PN.	1	L1

END OF SEARCH HISTORY

9/976836

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L12: Entry 13 of 14 File: USPT Aug 15, 2000

US-PAT-NO: 6105010
DOCUMENT-IDENTIFIER: US 6105010 A

TITLE: Biometric certifying authorities

DATE-ISSUED: August 15, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Musgrave; Clyde	Frisco	TX		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
GTE Service Corporation	Irving	TX			02

APPL-NO: 09/ 001323 [PALM]
DATE FILED: December 31, 1997

PARENT-CASE:
This application claims benefit of provisional applications 60/046,012, filed May 9, 1997, 60/067,182, filed Dec. 1, 1997 and 60/055,534, filed Aug. 13, 1997.

INT-CL: [07] G06 F 17/60

US-CL-ISSUED: 705/44; 705/39, 380/23, 380/25, 382/115
US-CL-CURRENT: 705/44; 380/255, 382/115, 705/39

FIELD-OF-SEARCH: 705/1, 705/39, 705/44, 380/23, 380/25, 382/115-119

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	4109237	August 1978	Hill	382/117
□	4405829	September 1983	Rivest et al.	380/30
□	5214699	May 1993	Monroe et al.	380/23
□	5224173	June 1993	Kuhns et al.	382/116
□	5259025	November 1993	Monroe et al.	380/23
□	5291560	March 1994	Daugman	382/117

□	5386104	January 1995	Sime	235/379
□	5412727	May 1995	Drexler et al.	380/24
□	5428357	June 1995	Haab et al.	341/155
□	5457747	October 1995	Drexler et al.	380/24
□	5469506	November 1995	Berson et al.	380/23
□	5534855	July 1996	Shockley et al.	340/825.3
□	5581630	December 1996	Bonneau, Jr.	382/116
□	5619620	April 1997	Eccles	706/20
□	5623545	April 1997	Childs et al.	708/250
□	5719950	February 1998	Osten et al.	382/115
□	5748738	May 1998	Bisbee et al.	380/25
□	5787186	July 1998	Schroeder	382/115
□	5838812	November 1998	Pare, Jr. et al.	382/115
□	5892838	April 1999	Brady	382/115
□	5905807	May 1999	Kato et al.	382/118

ART-UNIT: 274

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Nguyen; Cuong H.

ATTY-AGENT-FIRM: Suchyta; Leonard Charles

ABSTRACT:

A biometric certifying authority (BCA) management system and method provide and maintain a hierarchical relationship among biometric certifying authorities in the issuance of biometric certificates. Biometric certificates may be used in all electronic transactions requiring authentication of the participants, based on the accuracy and uniqueness of the biometric, which allows the electronic transaction to be insured to provide global standards for all electronic commerce. The BCA management system includes a transaction request parser which extracts a biometric certificate signal and transaction-type data from a electronic transaction request. A biometric verification processor verifies the biometric certificate signal against previously stored biometric data in a database. The biometric verification processor generates a verification message corresponding to the authenticity or fraudulent status of the biometric certificate signal. A transaction type classifier receives the electronic transaction request, and generates a classification message according to the transaction-type data. A certifying authority processor generates an access-or-denial message to indicate the status of the electronic transaction, and to report the classification of the transaction request.

20 Claims, 2 Drawing figures

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L12: Entry 13 of 14 File: USPT Aug 15, 2000

DOCUMENT-IDENTIFIER: US 6105010 A
TITLE: Biometric certifying authorities

Application Filing Date (1):
19971231

DATE ISSUED (1):
20000815

Brief Summary Text (3):
This disclosure relates generally to the field of secure communications, and in particular to the issuance and management of biometric certificates in a hierarchy of biometric security systems.

Brief Summary Text (5):
Electronic transactions may involve diverse types of activities, such as the exchange of information, the permitted entry and access of a person to a facility, and the output of goods or cash to a person. Despite the common need for security, different activities may have different levels of security, and so different activities may utilized different security techniques.

Brief Summary Text (6):
Existing certifying techniques, such as personal certificates employing, for example, passwords and personal information numbers (PINs), have not provided sufficient security since PINs and passwords are often easily guessed, hard to remember, and/or subject to exhaustive or brute-force automated searches.

Brief Summary Text (9):
Recently, access to electronic services has been facilitated through identification and security techniques using biometric certificates, such as described in U.S. patent application No. 60/046,012, entitled "BIOMETRIC CERTIFICATES" by Clyde Musgrave et al., which is incorporated herein by reference. Such biometric certificates are useful to authenticate the identity of a person and to bind the biometric of the person to a transaction via a digital certificate. Such biometric certificates may be used as a spoof-proof method for recognizing individuals within an end-to-end secure electronic transaction.

Brief Summary Text (10):
As different electronic transactions may require different levels of security, a need exists for controlling the generating, distributing, revoking, and maintaining of biometric certificates through one or more biometric certifying authorities (BCAs). Such a BCA control system should provide insurability of issued biometric certificates for different electronic transactions.

Brief Summary Text (12):
It is recognized herein that a hierarchical approach and evaluation procedure for the issuance of biometric certificates insures specific levels of security for specific types of electronic transactions.

Detailed Description Text (2):

Referring in specific detail to the drawings, with common reference numbers identifying similar or identical elements, steps, and features, as shown in FIG. 1, the present disclosure describes a biometric certifying authority management system and method of use for providing and maintaining a hierarchical relationship among biometric certifying authorities in the issuance of biometric certificates. The hierarchical approach and evaluation procedure in the issuance of biometric certificates insures specific levels of security for specific types of electronic transactions.

Detailed Description Text (10):
The transaction type data 20 is sent from the request parser 16 to a transaction type classifier 30 to determine the type of transaction and the corresponding level of security required of the transaction, according to a predetermined hierarchy shown, for example, in FIG. 2. The transaction request 14 may include a transaction code as the transaction type data 20 for indicating the type of transaction involved. The transaction type classifier 30 may then compare the transaction code with a set of predetermined transaction codes which may be stored, for example, in a transaction code table or database. The transaction type classifier 30 may then generate a security level code which is output to the certifying authority processor 28.

Detailed Description Text (11):
Upon receiving the verification message 26 and/or the security level code, the certifying authority processor 28 generates a response to the transaction requester 12. If the verification message 26 indicates authentication of or a failure to authenticate the biometric certificate 18, the certifying authority processor 28 generates an access or denial message 32, respectively. In one embodiment, the access or denial message 32 is sent to the transaction requester 12 for further processing of the transaction request 14. The access or denial message 32 may merely be a logic 1 or TRUE Boolean value indicating access granted, or a logic 0 or FALSE Boolean value indicating a denial of access. Alternatively, the access or denial message 32 may include a report on confidence of the authenticity, such as a percentage value indicating the percentage of confidence in the authenticity for an access indication, or lack thereof for a denial indication.

Detailed Description Text (13):
In conjunction with or independent of the access or denial message 32, the certifying authority processor may access a billing rate database 34 for generating a bill 36 or charge for the process of verifying and/or for providing a report on the confidence of the authentication or lack thereof. The billing rate database 34 may also include a table or database of insurance rates for charging the transaction requester 12, in the bill 36, to indicate a level of insurance commensurate with a level of security insured by a positive authentication by the BCA manager 10. Alternatively, the billing rate database 34 may specify a percentage of the transaction amount or value involved.

Detailed Description Text (15):
The bill 36 with the insurance charge may be in the form of a credit card transaction pre-authorized by the transaction requester 12 as a pre-established authentication and insurance service with the BCA manager 10. In this manner, the BCA manager 10 exchanges guarantees of authentication for payment of insurance and/or authentication charges, and so electronic transactions may be conducted with greater assurance of security and authenticity.

Detailed Description Text (16):
As shown in FIG. 2, the transaction type classifier 30 may classify transactions from different BCAs according to the predetermined hierarchy 38 of electronic transactions and BCAs conducting such electronic transactions. For example, all BCAs shown in FIG. 2 may be associated with a root BCA 40 having the highest degree of security. The root BCA 40 may have associated therewith electronic transactions

involving governmental and national security BCAs 42 as well as various digital and biometric certifying authority administrative BCAs 44. Such BCAs merit the greatest levels of security and correspondingly the greatest security values, since such BCAs 42, 44 involve agencies and systems which monitor and secure other electronic systems such as other BCAs.

Detailed Description Text (17):
For example, on a scale of 1 to 10, the BCAs 42, 44 in the root BCA 40 may be assigned a security value of 10, requiring the greatest accuracy in authentication of biometric certificates in electronic transactions.

Detailed Description Text (18):
The next lower level of the hierarchy 38 includes electronic fund transfer BCAs 46 such as banking BCAs 48 and securities BCAs 50 for providing biometric certificates involved in secure electronic transactions of money, money-related entities, and money-related information. On a scale of 1 to 10, the electronic fund transfer BCAs 46 may be assigned a security value of 8.

Detailed Description Text (19):
The next lower level of the hierarchy 38 includes insurance transaction BCAs 52 such as bonding BCAs 54 and surety BCAs 56 for providing biometric certificates for secure electronic transactions involving, for example, insurance and guarantee payment contracts. On a scale of 1 to 10, the insurance transaction BCAs 52 may be assigned a security value of 6.

Detailed Description Text (21):
lading, electronic letters of credit, etc. On a scale of 1 to 10, the business purchase BCAs 58 may be [redacted]

Detailed Description Text (22):
The next lower level of the hierarchy 38 includes physical security BCAs 64 such as automobile access BCAs 66 and door access BCAs 68 for providing biometric certificates for car doors, building and office doors, residences, etc. Such BCAs may be disposed at the physical location, such as being built into the body of an automobile, or may be remote such as being implemented by a central security station of an office building or laboratory. In addition, such physical security BCAs 64 may be implemented in airports and individual airplanes for use in or supplemental to the verification of alleged passengers prior to boarding an airplane. On a scale of 1 to 10, the physical security BCAs 64 may be assigned a security value of 2.

Detailed Description Text (23):
It is understood that the list of BCAs in the hierarchy 38 is not exhaustive and that the order of the BCAs may be implemented in different configurations, provided that each type of BCA is associated with a security value. In addition, individual BCAs within a specific type of BCA may be differentiated with unique or diverse security values. For example, within the electronic fund transfer BCAs 46, the banking BCAs may be assigned security values of 8.8 while the securities BCAs may be assigned security values of 8.4, such that banking transactions are required to be more secure than securities transactions, and so are charged more for authentication.

Detailed Description Text (24):
In addition, individual entities may request and/or pay the BCA manager 10 to set higher and/or lower security values. For example, instead of a security value of 8.8, an institution such as "CHASE MANHATTAN BANK" may pay a fee to have a security value of 9.5, to not only have greater security in electronic fund transfers but also to be able to advertise that their transactions are more secure than transactions of competitor banks. Alternatively, regulatory agencies may mandate that certain entities, such as banks, have a requisite minimum security level for

BCAs within the hierarchy 38. Further, such regulatory agencies may require certain entities advertise and otherwise inform consumers of the security ratings of transactions. For example, the Federal Trade Commission (FTC) may mandate that automobile makers, such as "FORD MOTOR COMPANY", inform automobile purchasers or renters that their "FORD" automobiles either lack a BCA system for physical security and access, or have a predetermined BCA security rating.

Detailed Description Text (25):
For businesses in general, there are about $10 million to about $100 million in fraud reserve funds collected and maintained annually. Business generally have about 100,000 to 500,000 electronic transactions per month, with fraud levels amounting from about $10 million to about $100 million annually. Generally, about 10,000 to 100,000 participants are involved in electronic transactions, with a market size greater than $1 billion per year. Accordingly, to implement BCA managers 10 and the BCA security hierarchy 38, businesses are clearly able to support the costs of biometric certificate hardware and software.

Detailed Description Text (42):
The security concerns of such electronic transactions is problematic, since there is generally a lack of uniform identification in large segments of the population. About $1 billion to $2 billion in check cashing transaction fees per year are collected, with fraud levels at about 10%.

Detailed Description Text (43):
The current needs of the marketplace involve check cashing facilities which take a portion of the face value or a fixed fee of each check cashed. The type of checks are typically government entitlement programs such Medicare, Medicaid, Social Security, Aid to Dependent Children, Food Stamps, Veteran's benefits, etc. The size of fraud in the Medicare and Medicaid programs alone is estimated at over $40 Billion. A portion of this fraud is attributable to check cashing fraud and lack of positive identification of the persons involved.

Detailed Description Text (52):
Biometric certificates fit well in this scenario, since biometric certificates create a new standard for secure identification (ID) methods. Electronic commerce in this scenario is keyed to cashless smartcards, with guaranteed security and insured validation of every transaction. Since cyberspace is relatively new, standards/laws for the cyberspace marketplace and commerce are evolving, and so cyberspace is ideal for experimenting with new paradigms.

Detailed Description Text (53):
The applications of biometric certificates using BCA managers 10 may be expanded to the government and the population, delivering biometric certificate security benefits after prototyping with the un-banked. Higher-value transactions may then be built and implemented, with nominal fees being charged such as $1.00 to $2.00 per transaction.

Detailed Description Text (70):
The needs of the marketplace for biometric certificates for subscription services include allowing customers to order products on credit electronically through a private network. The size of fraud in such subscription services is virtually unknown, but the approximate fraud exposure is about $10 million to $100 million. The lack of security prevents these companies from putting new and more valuable products up on their private networks. By putting new products up in a system with mutual trust using biometric certificates and the BCA manager 10, these companies are able to increase their per-transaction revenue and build a larger

CLAIMS:

1. A biometric certifying authority (BCA) management system comprising:

a transaction request parser for receiving a request to authenticate an electronic transaction having transaction-type data and a biometric certificate signal, the request parser operating to extract the biometric certificate signal and the transaction-type data from the request;

a biometric verification processor which receives the biometric certificate signal, determines an authenticity of the biometric certificate signal based on previously stored biometric data in a database, and based on the determination, generates a verification comprising one of an authentic status and a fraudulent status of the biometric certificate signal;

a transaction type classifier for receiving the transaction type data and for determining a security level associated with the electronic transaction based on at least one of the transaction-type data and a predetermined hierarchy of electronic transactions; and

a certifying authority processor for generating an access-or-denial message based on at least one of the verification and the security level.

3. The BCA management system of claim 1 wherein the predetermined hierarchy is a list of rankings of BCAs according to predetermined security and authentication levels.

5. The BCA management system of claim 4 wherein the billing rate database stores billing rates which increase for corresponding transaction classifications having greater associated security and authentication levels.

7. A biometric certifying authority (BCA) management system for authenticating an electronic transaction request, including a biometric certificate signal and transaction-type data, comprising:

a biometric verification processor which receives a biometric certificate signal, verifies the biometric signal based on biometric data in a database, and generates a verification comprising one of an authentic status and a fraudulent status of the biometric certificate signal;

a transaction type classifier which receives the request and generates a security level associated with the electronic transaction based on at least one of the transaction-type data and a predetermined hierarchy of electronic transactions;

a billing rate database which stores a plurality of billing rates corresponding to a plurality of security levels; and

a certifying authority processor for generating an access-or-denial message based on at least the verification, the certifying authority processor further operative to retrieve a corresponding billing rate from the billing rate database, and to generate a bill in accordance with the billing rate for the access-or-denial message.

10. The BCA management system of claim 9 wherein the billing rate database stores billing rates which increase for corresponding transaction classifications having greater associated security and authentication levels.

11. The BCA management system of claim 7 wherein the predetermined hierarchy is a list of rankings of BCAs according to predetermined security and authentication levels.

12. The BCA management system of claim 11 wherein the predetermined hierarchy includes rankings of BCAs from a group including at least one of: root BCAs,

electronic fund transfer BCAs, insurance BCAs, business purchase BCAs, and physical security BCAs.

16. The method of claim 15 wherein the predetermined hierarchy is a list of rankings of biometric certifying authorities (BCAs) according to predetermined security and authentication levels.

17. The method of claim 16 wherein the predetermined hierarchy includes rankings of BCAs from a group including at least one of: root BCAs, electronic fund transfer BCAs, insurance BCAs, business purchase BCAs, and physical security BCAs.

19. The method of claim 13 wherein the step of storing includes the step of storing billing rates in the billing rate database, with the billing rates increasing for corresponding transaction classifications having greater associated security and authentication levels.

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#

End of Result Set

□ Generate Collection Print

L1: Entry 1 of 1 File: USPT Sep 12, 2000

US-PAT-NO: 6119096
DOCUMENT-IDENTIFIER: US 6119096 A

TITLE: System and method for aircraft passenger check-in and boarding using iris recognition

DATE-ISSUED: September 12, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Mann; Stewart	Falls Church	VA		
Mann; L. Maribel	Falls Church	VA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
EyeTicket Corporation	McLean	VA			02

APPL-NO: 09/ 053216 [PALM]
DATE FILED: April 1, 1998

PARENT-CASE:
This application claims the benefit of the following U.S. Provisional Patent Applications: Ser. No. 60/070,566, filed Jan. 6, 1998, and Ser. No. 60/054,339, filed Jul. 31, 1997.

118-119
124

INT-CL: [07] G06 F 17/60

115
118-119
124

US-CL-ISSUED: 705/5; 382~~/117,~~ 235/384, 705~~/40~~
US-CL-CURRENT: 705/5; 235/384, 382/117, 70~~5/40~~

16,18

FIELD-OF-SEARCH: 705/35, 705/5, 705/40, 705/41, 705/42, 705/43, 705/44, 705/26, 705/27, 235/380, 235/384, 382/115, 382/116, 382/117, 382/118, 382/119, 382/124, 707/3, 707/4, 707/5, 707/6, 707/7, 707/9, 707/10

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
□	4210899	July 1980	Swonger et al.	382/117
□	4641349	February 1987	Flom et al.	382/125

□	4711994	December 1987	Greenberg	235/384
□	4798942	January 1989	Aubrey	235/384
□	5051565	September 1991	Wolfram	235/384
□	5053608	October 1991	Senanayake	235/380
□	5177342	January 1993	Adams	235/379
□	5225990	July 1993	Bunce et al.	700/226
□	5229764	July 1993	Matchett et al.	340/825.34
□	5280527	January 1994	Gullman et al.	713/184
□	5291560	March 1994	Daugman	382/117
□	5336870	August 1994	Hughes et al.	235/379
□	5469506	November 1995	Berson	713/186
□	5471203	November 1995	Sasaki et al.	340/825.31
□	5478993	December 1995	Derkson	235/380
□	5485520	January 1996	Chaum et al.	705/74
□	5497430	March 1996	Sadovnik et al.	382/156
□	5566327	October 1996	Sehr	707/104
□	5572596	November 1996	Wildes et al.	382/117
□	5578808	November 1996	Taylor	235/380
□	5594806	January 1997	Colbert	382/115
□	5613012	March 1997	Hoffman et al.	382/115
□	5615277	March 1997	Hoffman	382/115
□	5712914	January 1998	Aucsmith et al.	380/30
□	5764789	June 1998	Pare, Jr. et al.	392/115
□	5793639	August 1998	Yamazaki	700/226
□	5801367	September 1998	Asplund et al.	235/384
□	5809480	September 1998	Chasek	705/13
□	5845692	December 1998	Kellem et al.	160/118
□	5866888	February 1999	Bravman et al.	235/375
□	5877484	March 1999	Hirose	235/382
□	5901238	May 1999	Matsushita	382/117
□	5912981	June 1999	Hansmire et al.	382/116
□	5920053	July 1999	DeBrouse	235/375
□	5930761	July 1999	O'Toole	705/5
□	5943651	August 1999	Oosawa	705/5
□	5953440	September 1999	Zhang et al.	705/5
□	5953705	September 1999	Oneda	382/117
□	5956122	September 1999	Doster	351/210
	5978494	November 1999	Zhang	382/117

□				
□	5991429	November 1999	Coffin et al.	382/118

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0271022	June 1988	EP	
04063785	October 1993	JP	

OTHER PUBLICATIONS

Anonymous, "Smart cards promise multiple travel benefits", Jane's Airport Review, pp. 35, Mar. 1, 1996.
Torbenson, Eric, "Northwest Airlines to Upgrade Computers, Offer Self-Service Check-In," Knight Ridder Tribune Business News, Jul. 31, 1999.
Torbenson, Eric, "Airlines to Offer Faster Services to Attract Passengers," Knight-Ridder Tribune Business News, Jul. 31, 1999.
Hildreth, Elizabeth, "A Smart Biometric Answer for Airline Safety," Card Technology, Oct. 1, 1999, p. 27+, Faulkner & Gray, Inc.
"SITA at 50," Air Transport World, Jun. 1999, p. 51+, vol. 36 No. 6, Penton Publishing, Inc.
Broderick, Sean, "IATA, IBM to Offer Easy Link for E-Ticket Systems," Inside IT, Aug. 25, 1999, p. 1, vol. 1 No. 8, McGraw-Hill Companies, Inc.
Strassberg, Dan, "Biometrics: You are Your Password," EDN, May 7, 1998, p. 46(8), vol. 43 No. 10, Cahners Publishing Co.
"A Casual Look by Commuters May Mean the End of Tokens, Tickets Passes and Cash in Mass Transit," PR Newswire, Mar. 28, 1998, Spring Technologies, Inc.
Butterworth-Hayes, Philip, The Pitfalls and Promises of Self-Service Check-In Kiosks, Jane's Airport Review, Jan. 1, 1999, p. 46, vol. 11 No. 1.
"Facing Up to Biometrics: New report shows how Biometric Technologies will Change People's Lives," PR Newswire, Aug. 5, 1998, London, UK.
"The Eyes Have It," Electronic Payments International, Jan. 1998, p. 13, No. 126, Lafferty Publications Ltd.
Arnst, Catherine "Face to Face with the Latest in Airport Security," Jun. 2, 1997, Business Week, p. 130E, No. 3529, Mcgraw-Hill Companies, Inc.
McRae, Hamesh, "Business (A traveller's cheque for the future)," Independent on Sunday, Aug. 3, 1997.
"Airport Feature--The Intelligent Airport," Jane's Airport Review, May 1, 1996, p. 51, vol. 8 No. 4, Jane's Information Group.
Zutell, Irene, "Newark News: With Twice as much Space and Services, Newark's International Terminal Simplifies Transfers for Travelers," Travel Agent, Apr. 22, 1996, p. 26, Gale Group.
Churchill, David, "The Airlines' First Priorities (international business travelers)," Management Today, Oct. 1995, p. 90(4), Management Publications Ltd., UK.
"CDSI Unveils Biometric Smart Card System, Boosting Airport, Airline Security," PR Newswire, Aug. 17, 1995, p. 817DC017, Computer Data Systems, Inc., Rockville, Maryland.
Glauberman, Stu, "Proposed Airport Service would Speed up Arrivals," Honolulu Advertiser, Apr. 1, 1995, p. C-1.
Bredemeier, Judi, "Traveler or Terrorist?: High-Tech Passenger Profiling May Aid Airport Security," Business Travel News, Mar. 23, 1992, p. 1, Miller Freeman, Inc.

ART-UNIT: 271

PRIMARY-EXAMINER: Voeltz; Emanuel Todd

ASSISTANT-EXAMINER: Kalinowski; Alexander

ATTY-AGENT-FIRM: Smith; Evan R.

ABSTRACT:

A system and method for automated aircraft boarding uses an iris recognition system for check-in and boarding. The passenger is enrolled once and assigned an account number. The passenger thereafter makes reservations using that account number. On arrival at the airport, the passenger is identified using an iris recognition system and automatically checked in for the flight, without the use of cards or other identification. Entry to the aircraft at the gate may also be provided with an iris recognition station. In one preferred embodiment, baggage check and baggage reconciliation are also performed using iris recognition. In its preferred embodiment, the disclosed system and method enhances customer convenience by eliminating tickets, boarding passes, and identification steps, while improving aircraft security.

67 Claims, 14 Drawing figures

Previous Doc Next Doc Go to Doc#

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☒ 3. Document ID: US 20020174010 A1

L7: Entry 3 of 10 File: PGPB Nov 21, 2002

PGPUB-DOCUMENT-NUMBER: 20020174010
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020174010 A1

TITLE: System and method of permissive data flow and application transfer

PUBLICATION-DATE: November 21, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Rice, James L. III	Minneapolis	MN	US	

US-CL-CURRENT: 705/14

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

□ 4. Document ID: US 20020095357 A1

L7: Entry 4 of 10 File: PGPB Jul 18, 2002

PGPUB-DOCUMENT-NUMBER: 20020095357
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020095357 A1

TITLE: System and method permitting customers to order selected products from a vast array of products offered by multiple participating merchants and related security applications

PUBLICATION-DATE: July 18, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Hunter, Charles Eric	Hilton Head Island	SC	US	
Ballou, Bernard L. JR.	Raleigh	NC	US	
Summer, Robert D.	New Preston	CT	US	
Sparks, Kelly C.	Raleigh	NC	US	
Sykes, Ollin B.	Edenton	NC	US	
Hebrank, John H.	Durham	NC	US	

US-CL-CURRENT: 705/27

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

□ 5. Document ID: US 20010019604 A1

L7: Entry 5 of 10 File: PGPB Sep 6, 2001

PGPUB-DOCUMENT-NUMBER: 20010019604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20010019604 A1

TITLE: Enhanced communication platform and related communication method using the platform

PUBLICATION-DATE: September 6, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Joyce, Simon James	Bangkok	CO	TH	
Gupta, Prafulla C.	Pagosa Springs		US	
Vaidya, Manohar S.	Hyderabad		IN	
Alla, Rajesh	Hyderabad		IN	
Reddy, Ashok K.	Hyderabad		IN	
Ayyala, Sree Ram Murthy	Secunderabad		IN	
Gupta, Richa	Hyderabad		IN	
Kaushal, Alok	Hyderabad		IN	
Verma, J.S.J.L.K.	Hyderabad		IN	
Undavalli, Prasad	Hyderabad		IN	
Nallajerla, Kondal Rao	Secunderabad		IN	
Bonajiri, Sivaramayya	Secunderabad		IN	
Sistla, Krishna Mohan	Hyderabad		IN	
G., Amba Prasad	Hyderabad		IN	
Ray, Biswajit Sundar	Secunderabad		IN	
Govind, Raghuram	Hyderabad		IN	
Raju, Janaki Rama	Hyderabad		IN	
Rao, K. Veerabhadra	Hyderabad		IN	
Ravi, S. D. V.	Hyderabad		IN	
M. K., Ram Kumar	Secunderabad		IN	
Velpuri, Surya Sekhar	Hyderabad		IN	
Nallagonda, Bhanumurthy	Hyderabad		IN	

US-CL-CURRENT: 379/114.2; 379/144.01

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

□ 6. Document ID: US 6834195 B2

L7: Entry 6 of 10 File: USPT Dec 21, 2004

US-PAT-NO: 6834195
DOCUMENT-IDENTIFIER: US 6834195 B2

TITLE: Method and apparatus for scheduling presentation of digital content on a personal communication device

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

□ 7. Document ID: US 6381316 B2

L7: Entry 7 of 10 File: USPT Apr 30, 2002

US-PAT-NO: 6381316
DOCUMENT-IDENTIFIER: US 6381316 B2

TITLE: Enhanced communication platform and related communication method using the platform

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

□ 8. Document ID: US 6320947 B1

L7: Entry 8 of 10 File: USPT Nov 20, 2001

US-PAT-NO: 6320947
DOCUMENT-IDENTIFIER: US 6320947 B1

TITLE: Telephony platform and method for providing enhanced communication services

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

□ 9. Document ID: US 5950543 A

L7: Entry 9 of 10 File: USPT Sep 14, 1999

US-PAT-NO: 5950543
DOCUMENT-IDENTIFIER: US 5950543 A

TITLE: Evacuated tube transport

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

□ 10. Document ID: US 4895518 A

L7: Entry 10 of 10 File: USPT Jan 23, 1990

US-PAT-NO: 4895518
DOCUMENT-IDENTIFIER: US 4895518 A

TITLE: Computerized diagnostic reasoning evaluation system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

Clear Generate Collection Print Fwd Refs Bkwd Refs Generate OACS

Terms	Documents
L6 and rating	10

Display Format: - Change Format

Previous Page Next Page Go to Doc#

First Hit Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L7: Entry 3 of 10 File: PGPB Nov 21, 2002

DOCUMENT-IDENTIFIER: US 20020174010 A1
TITLE: System and method of permissive data flow and application transfer

Application Filing Date:
20010525

Detail Description Paragraph:
[0089] In service-oriented societies and economies, it is generally desirable to provide improved service to users. This improved service may be provided, in one embodiment of the subject invention, by providing wide-ranging access to free software. Service may also be improved by provision of means to provide certain businesses with an opportunity to better serve the primary registered users of this system and these methods also comprises an improved service, when desired, to the primary users. For example, the ability to better understand the customer's personal tastes and functional needs and to then maintain that information in a data warehouse is very valuable to businesses which may serve users of the present invention. The value of this information to businesses may make possible a reduced or free price in many instances, for the underlying information in the form of applications and other useful software to the primary user. In similar fashion, the data warehouse relating to many peoples' personal taste and functional needs is then able to be used in a manner to provide optimum service to the primary users. One example includes access to a frequent flyer's personal database by as many airlines as desire such information in order to greet the flying passenger upon boarding the aircraft with a customized product such as individually tailored meals, drinks, and newspapers and magazines to allow that passenger to enjoy the best possible service while onboard that particular aircraft. Once again, no longer is it a requirement that the passenger be a registered member of a plurality of airline programs nor is it any longer a requirement, after use of Applicant's invention, for each individual airline or air carrier to maintain distinctly different programs of exceptional, customized service to frequent passengers. Rather, such airlines may simply access the personalized database warehouse and utilize the more particular and specialized data on passengers or corporations to which service is to be provided. It is recognized that vendors and other service providers may also provide fee or other revenue or resources to such an online service described by Applicant when such vendors or others gain business opportunities via the business methods, techniques, and systems described herein.

Detail Description Paragraph:
[0095] Thus, for various types of software applications, a combination of a thin client mode and a fat client mode, or transition between thin client mode to fat client, is highly desirable. Examples of situations in which this combination may be useful include collaboration sessions among various team members on a project remotely located from each other but desirous of collaborating using both relatively small programs as well as a large program suitable to a web based application or simultaneous use, such as a large computer-aided design (CAD) program, an advanced scheduling program, or other advanced and relatively large-scale software programs. Indeed, this system may also incorporate utilization monitoring means for automatically entering a suitable mode, or by prompting users as to the optimum use mode to be in, as well as record such use, if desired, for later use. A collaboration session is preferably initiated by various users

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 10 of 14 returned.

□ 1. Document ID: US 20020025490 A1

Using default format because multiple data bases are involved.

L12: Entry 1 of 14 File: PGPB Feb 28, 2002

PGPUB-DOCUMENT-NUMBER: 20020025490
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020025490 A1

TITLE: Raman-active taggants and their recognition

PUBLICATION-DATE: February 28, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Shchegolikhin, Alexander Nikitovich	Moscow	CO	RU	
Lazareva, Olgal Leonidovna	Moscow		RU	
Melnikov, Valery Pavlovich	Moscow		RU	
Ozeretski, Vassili Yu	Moscow		RU	
Small, Lyle David	Peyton		US	

US-CL-CURRENT: 430/270.15; 283/90, 430/270.11, 430/270.14, 430/945

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

□ 2. Document ID: US 20020025062 A1

L12: Entry 2 of 14 File: PGPB Feb 28, 2002

PGPUB-DOCUMENT-NUMBER: 20020025062
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020025062 A1

TITLE: Method for identity verification

PUBLICATION-DATE: February 28, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Black, Gerald R.	Southfield	MI	US	

US-CL-CURRENT: 382/116

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

□ 3. Document ID: US 6721713 B1

L12: Entry 3 of 14 File: USPT Apr 13, 2004

US-PAT-NO: 6721713
DOCUMENT-IDENTIFIER: US 6721713 B1

TITLE: Business alliance identification in a web architecture framework

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

---

□ 4. Document ID: US 6629081 B1

L12: Entry 4 of 14 File: USPT Sep 30, 2003

US-PAT-NO: 6629081
DOCUMENT-IDENTIFIER: US 6629081 B1
**** See image for <u>Certificate of Correction</u> ****

TITLE: Account settlement and financing in an e-commerce environment

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

---

□ 5. Document ID: US 6615166 B1

L12: Entry 5 of 14 File: USPT Sep 2, 2003

US-PAT-NO: 6615166
DOCUMENT-IDENTIFIER: US 6615166 B1

TITLE: Prioritizing components of a network framework required for implementation of technology

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

---

□ 6. Document ID: US 6610351 B2

L12: Entry 6 of 14 File: USPT Aug 26, 2003

US-PAT-NO: 6610351
DOCUMENT-IDENTIFIER: US 6610351 B2

TITLE: Raman-active taggants and their recognition

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

□ 7. Document ID: US 6587835 B1

L12: Entry 7 of 14 File: USPT Jul 1, 2003

US-PAT-NO: 6587835
DOCUMENT-IDENTIFIER: US 6587835 B1

TITLE: Shopping assistance with handheld computing device

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw. De

□ 8. Document ID: US 6539101 B1

L12: Entry 8 of 14 File: USPT Mar 25, 2003

US-PAT-NO: 6539101
DOCUMENT-IDENTIFIER: US 6539101 B1
**** See image for Certificate of Correction ****

TITLE: Method for identity verification

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw. De

□ 9. Document ID: US 6536037 B1

L12: Entry 9 of 14 File: USPT Mar 18, 2003

US-PAT-NO: 6536037
DOCUMENT-IDENTIFIER: US 6536037 B1
**** See image for Certificate of Correction ****

TITLE: Identification of redundancies and omissions among components of a web based architecture

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw. De

□ 10. Document ID: US 6519571 B1

L12: Entry 10 of 14 File: USPT Feb 11, 2003

US-PAT-NO: 6519571
DOCUMENT-IDENTIFIER: US 6519571 B1
**** See image for Certificate of Correction ****

TITLE: Dynamic customer profile management

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw. De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L11 not L7	14

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs

Generate OACS

Search Results - Record(s) 11 through 14 of 14 returned.

□ 11. Document ID: US 6473794 B1

Using default format because multiple data bases are involved.

L12: Entry 11 of 14 File: USPT Oct 29, 2002

US-PAT-NO: 6473794
DOCUMENT-IDENTIFIER: US 6473794 B1

TITLE: System for establishing plan to test components of web based framework by displaying pictorial representation and conveying indicia coded components of existing network framework

DATE-ISSUED: October 29, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Guheen; Michael F.	Tiburon	CA		
Mitchell; James D.	Manhattan Beach	CA		
Barrese; James J.	San Jose	CA		

US-CL-CURRENT: 709/223; 709/224

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

□ 12. Document ID: US 6307956 B1

L12: Entry 12 of 14 File: USPT Oct 23, 2001

US-PAT-NO: 6307956
DOCUMENT-IDENTIFIER: US 6307956 B1

TITLE: Writing implement for identity verification system

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

□ 13. Document ID: US 6105010 A

L12: Entry 13 of 14 File: USPT Aug 15, 2000

US-PAT-NO: 6105010
DOCUMENT-IDENTIFIER: US 6105010 A

TITLE: Biometric certifying authorities

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

□ 14. Document ID: US 6074312 A

L12: Entry 14 of 14 File: USPT Jun 13, 2000

US-PAT-NO: 6074312
DOCUMENT-IDENTIFIER: US 6074312 A

TITLE: Golf handicap system and methods

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L11 not L7	14

Display Format: - Change Format

Previous Page Next Page Go to Doc#

accessing a single computer data file, such as a word processing document file. The document file, and any software required to view or edit the document file may be requested by a remote user by, for example, activating a hyperlink by clicking on a document name in an HTML document within the WWW application over the http protocol. This link would prompt the remote server to preferably download to the requesting user thin client software which, in combination with the information on the server pointed to by the AppLink about which file and application to open, allows the user to cause the server to start a file-compatible application, open the data file, and present the application to the remote user in thin-client mode according to the permissions granted to the user by, for example, the originator or other administrator of the document permissions information. The permissions granted to a user may preferably be altered on a dynamic basis, for example, where several users view a document at one time. In this instance, one user preferably will be granted write permission to the data file while all other users are granted a lesser form of permission such as "read". This provides version control to the data file and avoids problems with inconsistencies between what is ostensibly the same data file from the point of view of the users. In addition to limitations on user's rights to write, modify, or delete data files, the present invention preferably may be configured by a data file originator or administrator to allow other users to view a document, but withholding permission to the other user's to save the data file. The user may be presented with a screen showing various options for security and access provisions for a data file, e.g., a word processing file, spreadsheet file, or CAD drawing.

Detail Description Paragraph:
[0102] An example of the advantages of a combination thin-client/fat-client system and method comprises a user operating a portable computer in a public location, for example, near an airport departure lounge. In this instance, at a first moment in time the user is connected to a remote communications network, and is operating the relatively small memory capacity portable computer or laptop computer or hand held or palm size computing device in the thin client mode to optimize availability of advanced programs without the requirement to dominate use of the remaining available portion of memory in the local computing device. However, as the user's aircraft boarding time approaches it may be desirable for the user to employ signal means to shift from a thin client mode to a fat client mode for a selectable portion of an application desired for use onboard the aircraft, but which is not then resident on the user's computing device. This scenario corresponds to the "termination of communications imminent" branch 132 of the state diagram 108 diagram of FIG. 1. This technology and methodology, therefore, permits such a user to optionally select mode shifts between the client user modes in order to optimize not only the computing device memory ratio to software utilized but also to take into account and to accommodate situational elements which occur every day worldwide and which heretofore have not been dealt with in a manner that permits seamless utilization of the computing device in the various situations. In the above example, the user may optionally choose to return to the thin client mode indicated as event 134 in state diagram 108, possibly in the same application program, upon arrival at her destination.

Detail Description Paragraph:
[0104] In addition to personal databases and business databases, it is possible to provide collaboration tools, file storage means, office suite programs and other types of desirable packages to the computing device user, such as premium channel packages. The advantages of using the systems and methods described herein include resource savings including financial savings, time savings, ready access throughout the world, minimization or eradication of synchronization problems in various interface scenarios, improved data security due to a reduction in data resident to highly portable and easily lost or stolen portable computing devices, enhanced team productivity among multiple users, dramatically improved session persistence of users, ready access at one logon or communications step to vast stores of information which may have previously required multiple communication access steps

and other advantages. The experience of a user under this communication system thus duplicates a virtual private network, and may be experienced as fully interconnected network 190 of FIG. 4.

Detail Description Paragraph:
[0111] One advantage of sending this hyperlink to a recipient in an e-mail compared to the alternative of simply including the file as an attachment to the e-mail is that there is no computer virus danger for the recipient. Many viruses are spread via e-mail attachments, and many companies have prohibited all e-mail attachments as a security risk. The thin client software required on the recipient's computer can be a "signed" Java applet, meaning that a central certifying authority has certified the thin client to be virus-free, and this single program is downloaded only once, versus multiple download/run cycles for e-mail file attachments. The application file hyperlink is a way to allow an employee of such a company to view and work with a file without having to receive the file in an attachment, or download it. Another advantage of this method for giving a user the ability to view and work with a file in a server-based application is that the originator can then be sure that the recipient will be able to view and work with the file, regardless of whether the recipient has a program capable of opening that file installed on his or her PC, since a server-based file-compatible application is, in a sense, sent along with the file. Viewing a file regardless of the application used to create it is also the function of ADOBE's PDF document format. With PDF, a PDF file is derived from a document by a conversion utility. This file is then sent as an attachment or download to the recipient, who then views it if he has the PDF viewer installed on his computer. PDF is essentially a "picture" of a document, meaning that the recipient cannot change it. With an application file hyperlink, the recipient has full capability to interact with the file. For example, a spreadsheet may have several embedded "macros" which would be inaccessible to a person viewing a PDF file. Or, a presentation delivered via AppLink can have full animation and sound. With PDF, a file is transferred to the recipient. With AppLink, no file is transferred, and it is not necessary that the recipient have a viewer installed on his machine, although he will need a compatible thin client. Another advantage is that access to data files of arbitrarily large size can be given to the recipient without sending the file itself, and without the necessity of the recipient ever downloading the file. Many Internet Service Providers have file attachment size limits of from one to five megabytes. An application file hyperlink bypasses that limit, since no file is sent. The thin client applet is typically under three megabytes in size. There are emerging numerous file conversion utilities and services which will convert various document formats into HTML, and display the document to the viewer in the form of a web page. This has the advantage of not sending the file to the recipient, but at a cost of removing any functionality from the document. This "HTML-Viewer" technique has problems with "multi-paged" files, such as a Microsoft Excel spreadsheet with 20 pages.

Detail Description Paragraph:
[0118] Altering application interfaces according to file metadata or user role may require rewriting the applications to respond to the interface specifications contained in the file metadata. However, there is a method to get this capability immediately by "fooling" the applications with false users, and using existing application interface modification capabilities. By having the file metadata present itself to the application as different users, and then using the application's existing interface modification capability to produce different user interfaces associated with each false user, it will be possible to use the existing personalization features of many programs to achieve different interfaces and functionality, which can then be directed to each user according to the user's permissions or security settings. For example, a file's application interface may have several optimal interfaces, depending on whether it is used in an AppLink, or which user accesses it. Each of those interfaces could be associated with a false user. This may be seen in the following table showing applicable relationships between file usage, the false usemame associated with a particular interface, and

the particular interface requirements.

Detail Description Paragraph:
[0131] In addition to the control of sensitive documents vis--vis employees, the application link of the present invention is preferably implemented in a manner by which the document control, e.g. as part of an IP management system, is extended to outside parties such as contractors or investors. Accordingly, in a preferred embodiment of the present invention, the application link is paired with an application link e-mail gateway to external parties. The application link e-mail gateway is preferably implemented to interface with several popular e-mail, or SMTP applications, e.g., Microsoft Exchange. The gateway is preferably configured to be consistent with both outgoing and incoming e-mails. The gateway according to the present invention may effect security functions in both outgoing and incoming e-mail. With regard to incoming mail, preferably all attachments contained in e-mails are intercepted by the application link e-mail gateway and stored to a central server. Ingoing message attachments are scanned for possible viruses. A dynamically created AppLink, which could be a URL, pointing to the attachment file on the server is inserted into the e-mail. The e-mail (without the attachment) is then forwarded to the recipient. To view and interact with the attachment via thin client, the recipient clicks on the AppLink and the attachment file is opened in a compatible server-based application.

Detail Description Paragraph:
[0132] For outgoing messages, the file security level is retrieved from the file metadata, as discussed above, and the appropriate restrictions are added to the application link. The recipient clicks on the application link hyperlink and the file is opened with the proper server-based application from the application link e-mail gateway server. The recipient then interacts with the file via thin client. The present invention assures that no files enter or leave an organization without authorization or central control. This is because external users accessing an application link only receive screenshots of the file and application. The file itself never leaves the corporate network, or preferably, the central server itself. Preferably, the application links are created automatically, so that end users do not have to change their behavior (e.g., with regard to sending attachments), and the centralized control afforded by the present invention cannot be defeated. As discussed above, access restrictions and application functionality restrictions can be created automatically based upon the file security level contained in the file metadata. This security level may, in turn, be tied to the sender's or recipient's job title or security clearance, in addition to file-specific criteria. Where multiple restriction criteria apply, the most restrictive choice can be made. For example, normally a document might have minimal restrictions, but because it is being sent to a potential competitor, access is severely limited.

Detail Description Paragraph:
[0133] The central file control afforded by the present invention may be used to effect internal IP control and document control. According to the present invention, an organization or individual may implement document security in a centralized manner. All sensitive files may be stored on one or more central servers. When accessing files, users click on a hyperlink to open the document in the proper application. Each user may be granted a security clearance level, for example, based upon rank, position, department, or other criteria. In addition to the user security level, each file preferably will also have a security level. The combination of the file security level and user security clearance level determine which files are available and the user's level of access. For example the user may or may not be able to edit, save, save as, print, copy, or the like, depending on their access. Similar security classifications may also be effected at the directory, or "folder" level. Directories of the files that are available, based upon the user's security clearance level or department, may be made available to the sending party, or the recipient or accessing party, to determine the files that

the recipient may link to. Therefore, the invention will preferably provide for storage navigation tools, e.g., a file manager or the like.

Detail Description Paragraph:
[0134] Preferably, in the event that a recipient does not have proper security classification for a document they are sent, a workflow component would be available for users to request increased access rights to a document from the sender or from another party with a suitable higher clearance level, for example, a supervisor or administrator.

Detail Description Paragraph:
[0135] In a preferred embodiment, efficient document searching is provided by an indexing system. Thus, the document library on the central server would be indexed so that a document may be searched by author, title, keywords, the permitted actions per security level, and the like. The documents in turn may be cataloged by similar or corresponding fields.

Detail Description Paragraph:
[0136] In a file distribution system according to the present invention, no files are ever stored on a user's PC or network access device. Instead, users of the AppLink Document Library only receive decrypted screenshots of the file and application. The file itself is never stored on their network access device/PC. This is linked with a dynamic security model determined by combination of file security level and user security clearance level.

Detail Description Paragraph:
[0138] For those files and applications for which the user's security admits, files and their native applications can be accessed by a central corporate office, a remote office, employees working from home, and traveling employees. In all cases, full security and encryption measures are in effect, which can be tracked and confirmed, and it may be ensured that derivative copies are not created. In a preferred embodiment, it is also possible that the "Save As" functionality of an application will not allow the user to create a new file, e.g., a document, that will have less restrictive security applications per user security level than the parent file.

Detail Description Paragraph:
[0139] Because the central server is the repository for all files in their native format, all files stored on the central server can be encrypted. In addition, all data, such as files, applications, and screen views of the remotely running application, that are delivered over the network to users can be encrypted. Delivery of files and applications over the network can be accomplished via a middleware environment comprising a middleware web-enabling application, e.g., Tarantella or Citrix, and application servers. Preferably, end-users receive primarily or solely, the screen shots of the document and application, the application executing on a central server. The AppLink security mechanism will interface with existing security approaches including existing or future encryption methods, such as PKI, 3DES, AES, or the like. These encryption methods may be symmetric or asymmetric. The AppLink security will also preferably be compatible with various user authentication or validation methods, including but not limited to passphrases, smart cards, token, fingerprint, retinal scan, or other biometric data.

Detail Description Paragraph:
[0140] Each file has metadata associated with it that specifies the security level of the file. Each user, in turn, has a specified clearance level. The file security level and the user clearance level interact or are compared in order to determine the user's access and privileges with the individual file. Applicable application functionality restrictions may include the following: read/write, read-only, no printing, no editing, no copying, or various other restriction on application

functions as applied to the particular file. The restrictions may also be event or time-based, e.g., there may be a restriction that a user may access the file a certain number of times, view until a particular date. The access may also be based on the access location of a remote user, e.g. a user may only access the file from a certain IP address or modem phone number, or conversely, may NOT access the file from certain IP addresses or phone numbers. This may prevent unauthorized access when authentication information is compromised, or during a duress situation, or to prevent applications from being used in countries where export laws prohibit use. In addition to business applications, allowing implementing organizations to ensure the confidentiality of internal or client projects, the present invention also admits of certain military and government applications. For example, the present invention may be used to prevent cases of espionage, or the unauthorized access or downloading of files in excess of one's authority. As another example, documents may be securely maintained on a central server, thus eliminating the problem of a stolen or misplaced laptop, for example, compromising the security of documents on the laptop. In the healthcare arena, the present invention may be used to implement the patient data protections mandated by the HIPAA statute and regulations. Data may be viewed securely by authorized users, without allowing the viewing, downloading, or further transmission of unauthorized patient information, thus aiding in compliance with regulations governing the security of individually-identifiable patient information.

Detail Description Paragraph:
[0155] FIG. 12 is a depiction of a process flow relating to the creation of a guest account for access to application link according to one embodiment of the present invention. As depicted in FIG. 12, the recipient of an AppLink will preferably be granted access to a temporary guest account created upon execution of the AppLink at 1212, following AppLink execution 1210. Alternatively, multiple guest account may be created in advance and assigned to specific AppLinks as they are activated. The AppLinked file may be copied from server-accessible storage at 1216 into the guest account 1218, and a compatible application may then open the copied file in the guest account. The creation of guest accounts for AppLink recipients may be expected to create a more secure system than the alternative of opening the AppLinked file within the account of the sender, with restrictive "guest" file access permissions, as depicted in FIG. 39, although this alternative can be advantageous for collaboration since it facilitates the AppLink sender viewing a document altered by a recipient, because it is contained in his account's readily accessible data storage. Since AppLinks can be transmitted to a broad range of recipients, some of whom might not be known to the sender or particularly trusted, security is vital. Accessing an AppLink with a "dummy" user account rather than directly from the AppLink creator's account (with file access restrictions, of course), the damage which an unscrupulous, "hacker" AppLink recipient could do may be restricted. For example, there would be no way for such a recipient to access or delete other files contained in an AppLink sender's service account. The temporary guest account may be automatically deleted 1220 upon termination of the session 1222.

Detail Description Paragraph:
[0166] AppLink restrictions on recipient actions may include the following: allow (or disallow) local printing; screen capture/print; local file save; AppLink server file save (modify base document); or allow/disallow local download. The settable variables may involve one or more of the following AppLink or file attributes, which may vary according to the degree of trust placed in the recipient, whether all recipients are known, the degree of sensitivity of the file, and the like. For example, variables may involve printing--the recipient may be allowed to print the file locally, in the case of a trusted recipient, or for an untrusted recipient, no printing is allowed. Similarly, the recipient may be allowed to use the "Print-Screen" capability of the local PC to print a screenshot of the file locally (trusted recipient) or not (untrusted recipient). The recipient may or may not be permitted to save the file locally or copy to a PC "clipboard" or similar memory

utility. This ability to prevent saving and printing may be expected to enhance the ability of the AppLink creator to protect any intellectual property or security of the AppLinked file by restricting copying and redistribution. In addition to setting restrictions on local saving of the AppLinked file, the creator will also preferably be able to specify whether downloading to the recipient's machine is permitted. This may be distinguished from the saving variable discussed previously, i.e., saving from the server-based application. When downloading is enabled, a link to a simple file download utility may be permitted. Downloading a file and opening it with an application running on the AppLink recipient's local PC is for many purposes inconsistent with the AppLink system. However, this download option will ensure file accessibility, as a backup system, if the sender was uncertain about whether the recipient could operate the required thin-client, perhaps due to the recipient being behind an incompatible firewall, or the recipient possibly accessing the AppLink from a computing device that has no thin client support at the time. The download capability would ensure that the recipient would get the file, albeit at the cost of losing control of it, and losing the certainty of whether the recipient could open it in a compatible application. Therefore, the AppLink creator would have to balance the need to ensure the AppLink recipient gets access to a file with the requirement to retain control of a file. Naturally, this option would only be given to trusted AppLink recipients. Other variables include the capability to Save Changes onto the AppLink Server, i.e., whether the AppLink recipient may change the document permanently and save the changes on the server. This may be among the variable settings "read-write" permissions to a trusted recipient, or "read only" permissions to an untrusted recipient.

Detail Description Paragraph:
[0182] The algorithm could also consider other applications for which the recipient has rights, and which are compatible with the file being AppLinked, but not necessarily the application used by the AppLink sender to create the file ("native application"). As a lower priority, a compatible "viewer" application with appropriate licensing could be selected, with the limitation that the user may not be able to interact with the file to the degree that he could if a fully capable native file application were used. This embodiment of the present invention, by which licensing impacts application functionality, may be implemented in conjunction with a previously-discussed embodiment, by which various application versions have different functionality in order to effect file permission security. That is, licensing terms may give differing levels of functionality for different payments to the vendor or different circumstances. A "demonstration" license might require disabled functionality.

Detail Description Paragraph:
[0220] Files may be provided with redundancy based on their importance. According to this embodiment, files may be assigned a centrally set variable redundancy based on individual file characteristics. An important file could be given, for example, a redundancy level of "5," meaning for example that 5 complete copies of the file or file set are available in different storage device locations. Finally, if a file is identified as having need for high security, the metafile server may move such file to a storage device having the requisite security parameters, according to the file security level rating or number assigned to the file or file type by a file or network administrator.

Detail Description Paragraph:
[0225] This Metafile System with Central Control may be further enhanced, according to an embodiment of the invention, through the use of Intelligent File Management, i.e., the ability of a Metafile System to integrate multiple SDs of varying performance, security, and cost presents new problems of optimization other than simply tracking file location. These variable characteristics of SDs are taken into account by intelligent file management rules that are designed to optimize these resources as follows: Central control is provided to an administrator via automatic file management rules for a Metafile System. According to this embodiment, optimal

file location may be set according to various Storage Device (SD) criteria such as storage cost or security; and/or according to file metadata such as usage/access frequency, importance, required security, file creator/owner, or setting the number of backup copies of a file according to it's importance and the availability and cost of backup storage space. In a specific embodiment of this Intelligent File Management, the ability to associate any type of metadata with a particular file is provided, allowing an administrator to specify rules for intelligent file management which would be carried out by the Metaserver.

Previous Doc Next Doc Go to Doc#

First Hit Previous Doc Next Doc Go to Doc#

□ Generate Collection Print

L7: Entry 5 of 10 File: PGPB Sep 6, 2001

PGPUB-DOCUMENT-NUMBER: 20010019604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20010019604 A1

TITLE: Enhanced communication platform and related communication method using the platform

PUBLICATION-DATE: September 6, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Joyce, Simon James	Bangkok	CO	TH	
Gupta, Prafulla C.	Pagosa Springs		US	
Vaidya, Manohar S.	Hyderabad		IN	
Alla, Rajesh	Hyderabad		IN	
Reddy, Ashok K.	Hyderabad		IN	
Ayyala, Sree Ram Murthy	Secunderabad		IN	
Gupta, Richa	Hyderabad		IN	
Kaushal, Alok	Hyderabad		IN	
Verma, J.S.J.L.K.	Hyderabad		IN	
Undavalli, Prasad	Hyderabad		IN	
Nallajerla, Kondal Rao	Secunderabad		IN	
Bonajiri, Sivaramayya	Secunderabad		IN	
Sistla, Krishna Mohan	Hyderabad		IN	
G., Amba Prasad	Hyderabad		IN	
Ray, Biswajit Sundar	Secunderabad		IN	
Govind, Raghuram	Hyderabad		IN	
Raju, Janaki Rama	Hyderabad		IN	
Rao, K. Veerabhadra	Hyderabad		IN	
Ravi, S. D. V.	Hyderabad		IN	
M. K., Ram Kumar	Secunderabad		IN	
Velpuri, Surya Sekhar	Hyderabad		IN	
Nallagonda, Bhanumurthy	Hyderabad		IN	

US-CL-CURRENT: 379/114.2; 379/144.01

ABSTRACT:

An advanced intelligent communication system that provides subscriber-requested, advanced communication services through existing communication switches even in those circumstances in which the hardware communication switch is not configured to provide such communication services. The system supports the use of personal identification number access cards for use in fixed and mobile markets from any communication device located anywhere in the world and provides flexible call

processing and switching services that deliver enhanced computer telephony capabilities utilizing standard communication equipment and operating systems.

Previous Doc Next Doc Go to Doc#

9/976836

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs
Generate OACS

Search Results - Record(s) 1 through 10 of 10 returned.

□ 1. Document ID: US 20040098154 A1

Using default format because multiple data bases are involved.

L7: Entry 1 of 10 File: PGPB May 20, 2004

PGPUB-DOCUMENT-NUMBER: 20040098154
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20040098154 A1

TITLE: Method and apparatus for computer system engineering

PUBLICATION-DATE: May 20, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
McCarthy, Brendan	Piano	TX	US	

US-CL-CURRENT: 700/97

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

---

□ 2. Document ID: US 20030063072 A1

L7: Entry 2 of 10 File: PGPB Apr 3, 2003

PGPUB-DOCUMENT-NUMBER: 20030063072
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030063072 A1

TITLE: Method and apparatus for scheduling presentation of digital content on a personal communication device

PUBLICATION-DATE: April 3, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Brandenberg, Carl Brock	Cresson	TX	US	
Kay, Robert L.	Fort Worth	TX	US	
Maxwell, Kenneth J.	Fort Worth	TX	US	
Cotter, R. Brandon	Dallas	TX	US	

US-CL-CURRENT: 345/173